FAA National Software Conference, June 2001
RTCA/SC-190

RTCA/SC-190

Ron Stroup

FAA, Office of Information Services

Process Engineering Division, AIO-200

(202) 493-4390

Ronald.L.Stroup@faa.gov

Terms of Reference

- Develop guidance material based on DO178B/ED12B for Communication, Navigation and Surveillance (CNS) and Air Traffic Management (ATM) software shown by system safety assessment [SC189/WG53-specified process] to affect the safety of aircraft occupants or airframe in its operational environment. Relevant software integrity assurance standards and approval processes should be taken into account.

Ron Stroup

FAA National Software Conference, June 2001
RTCA/SC-190

Philosophy

- The regulatory authorities and the aviation community to achieve a common DO/ED document for software considerations and assurance for airborne and CNS/ATM systems.

Schedule

- Plenary/Industry review - January 2001
- Plenary Web-vote/Resolve issues - March 2001
- Plenary Approved - April 2001
- RTCA/EUROCAE Ballot - July 2001
- Release: TBD (??November 2001??)

Ron Stroup

FAA National Software Conference, June 2001
RTCA/SC-190

Product

**Guidelines for CNS/ATM System
Software Integrity Assurance**

Outline (1/2)

- Introduction
  - Purpose
  - Scope
  - Relationship to other documents
  - document overview
  - How to use this document
- System Aspects Relating to CNS/ATM
  Software Development
  - Assurance levels
  - Additional system considerations

Ron Stroup

Outline (2/2)

- Objectives for CNS/ATM Systems
  - Annex A Tables
  - Considerations in applying Objectives to CNS/ATM systems
- Additional considerations
  - COTS
  - Adaptation
- CNS/ATM Life Cycle Data
- Acronyms and Glossary

Relationship to other documents

- Linked to DO-178B
  - Produce an equivalent level of software assurance between CNS/ATM and airborne systems
- Other assurance standards
  - Incompatibilities identified
- Other System Safety Assessment processes
  - WG53/SC-189 is an input to this document

Ron Stroup

How to use the document

- Read section one and three of DO-178B.
- Read DO-XX.
- Read section two and Twelve of DO-178B
  - Software Life Cycle

As questions in application arise, refer to the appropriate DO-178B text as referenced in the objectives tables and notes stated herein.
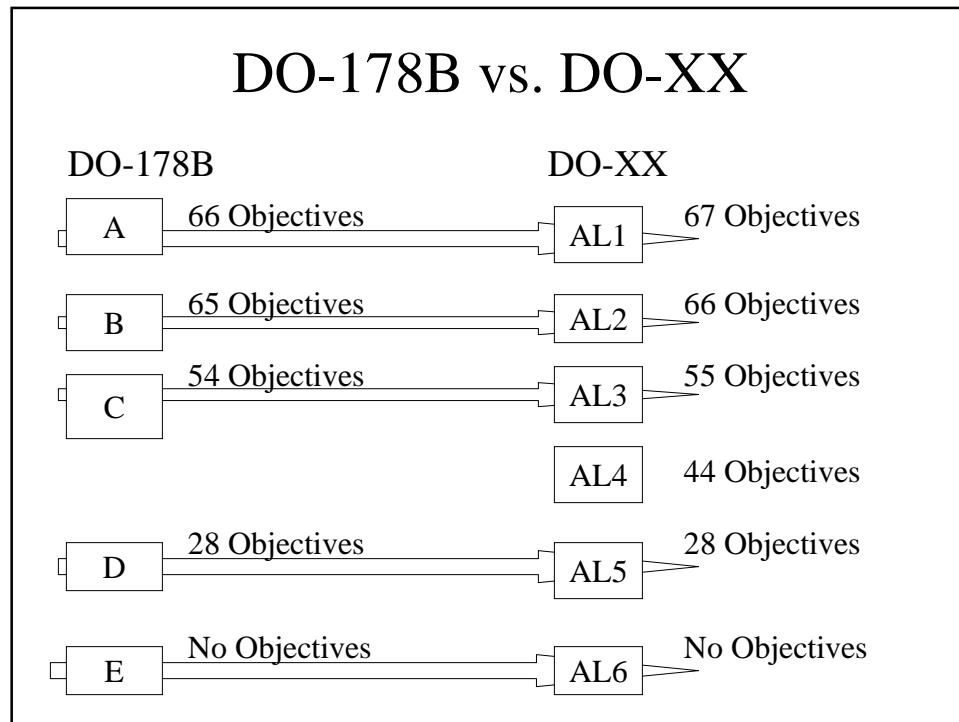
Assurance levels

- DO-XX/ED-XX
  - AL1
  - AL2
  - AL3
  - AL4
  - AL5
  - AL6

- DO-178B/ED-12B
  - A
  - B
  - C
  - Not Applicable
  - D
  - E

EQUIVALENCE

Ron Stroup

DO-178B vs. DO-XX

DO-178B DO-XX

A	66 Objectives	AL1	67 Objectives
B	65 Objectives	AL2	66 Objectives
C	54 Objectives	AL3	55 Objectives
		AL4	44 Objectives
D	28 Objectives	AL5	28 Objectives
E	No Objectives	AL6	No Objectives

Objectives

- Considerations
- Example
  - A1-3, Software life cycle environment is defined
    - Notes, CNS/ATM systems may have been in operation for many years, the software life cycle plans for these systems should include processes for software changes, technology upgrades, specifically with respect to safety issues.

Ron Stroup

Additional Considerations

- Issues

  - Site Adaptation Data
  - COTS

COTS

- Scope
  - Does not alter or substitute any of the objectives.
 - Accepted by approval authority

- 11 additional Objectives

COTS Process

- Planning
  - Activities are defined
  - Transition criteria is defined
  - Plans are consistent with CNS/ATM plans
- Acquisition
  - COTS capabilities determined.
  - Adequacy of Lifecycle data.
  - Compatibility with target hardware and other software
- Verification
  - Use existing verification objectives

COTS Acquisition Process

- Requirements Definition
- Assessment
- Selection

CNS/ATM Requirements

CNS/ATM Requirements satisfied by COTS

COTS Capabilities

Ron Stroup
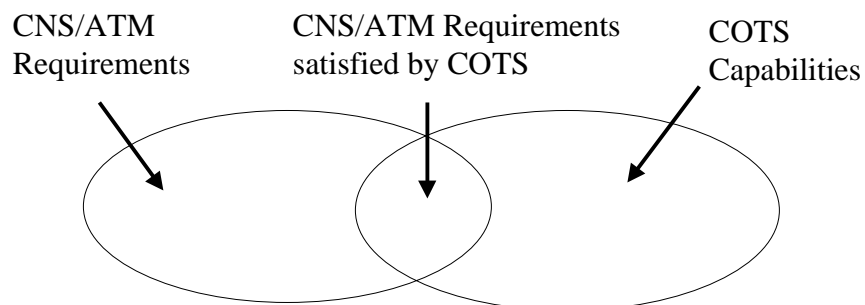
FAA National Software Conference, June 2001
RTCA/SC-190

Issues

- Scope - Data Link vs. CNS/ATM
- Safety Process - Bridging the gap between RTCA/SC-189 output and DO-178B required input.
- PDS/COTS - new objectives
- Independence

Example Issue

- Independence
  - Person, Department, and Organization
  - Increasing independence based of software level

FAA National Software Conference, June 2001
RTCA/SC-190

FAA Implementation of Software Assurance

WHAT

Adaptation
COTS

DO-XX
CNS/ATM

Objectives

DO-248B

DO-178B
Airborne

HOW

Maintenance
Safety/Security
iCMM/AMS
System aspects

FAA

Re-format

Ron Stroup